REMARKS

This Amendment is submitted in response to the Office Action dated April 7, 2004, having a shortened statutory period set to expire July 7, 2004. In the present Amendment, claims 2-3, 5, 11-13, 15-16, 18, 24-26, 28-29, 31, and 37-39 have been cancelled without prejudice, and claims 1, 4, 6-10, 14, 17, 19-23, 25-27, 30, and 32-36 have been amended. Claims 1, 4, 6-10, 14, 17, 19-23, 25-27, 30, and 32-36 are now pending.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-4, 7-10, 13-17, 20-24, 27-30, 33-36, and 39 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,304,969, issued to Wasserman et al. (*Wasserman* hereinafter) in view of U.S. Pat. No. 6,654,914, issued to Kaffine et al. (*Kaffine* hereinafter), in further view of U.S. Pat. No. 5,884,024, issued to Lim et al. (*Lim* hereinafter).

Regarding the grounds for rejecting independent claims 1, 14 and 27, Applicants agree that *Wasserman* discloses a method and system for verifying authorization of a server to provide network resources to a client. Specifically, the *Wasserman* verification process fundamentally relies on a server decryption of client generated messages with authorized servers having the required decryption key, which as explained below, is entirely unrelated to Applicants' claimed technique which relates more particularly to detection and subsequent active suppression of unauthorized configuration servers.

In further regard to the grounds for rejecting independent claims 1, 14 and 27, Applicants contend that *Kaffine's* vague and unsupported statement that "[t]he user and/or the network can be simulated to the other" does not disclose Applicants' proposed step of simulating a plurality of network clients within a server checker client. Furthermore, Applicants content there is no inherent or expressly described basis or motivation for combining the user/network simulation feature mentioned in passing by *Kaffine* with the decryption server authorization technique disclosed by *Wasserman*.

In further regard to the grounds for rejecting independent claims 1, 14 and 27, Applicants agree that *Lim* discloses a method and apparatus for reducing the probability of IP address misuse among *clients* of a DHCP server. As explained by Lim at col. 2, lines 28-34, one such problem is known as "IP address hogging" in which a client attempts to exhaust the supply of IP

·addresses by repeatedly obtaining IP leases from a DHCP server. Applicants contend however, that, absent Applicants' disclosure and claims, there is clearly a lack of motivation or suggestion in any of the foregoing references to combine a described problem (i.e. IP address hogging) as a constituent remedy feature in either *Wasserman* or *Kaffine*.

The foregoing contentions notwithstanding, independent claims 1, 14 and 27 have been amended to more clearly define and distinguish the subject matter of Applicants' proposed invention from the subject matter disclosed by the prior art. Specifically, amended claim 1 now recites a method for preventing unauthorized configuration servers from responding to client configuration requests in an IP network, including steps of: broadcasting host configuration requests from a server checker client; receiving configuration offer messages from one or more dynamic host configuration servers, said configuration offer messages delivered to the server checker client responsive to the broadcast host configuration requests; detecting an unauthorized dynamic host configuration server within said IP network in accordance with server identification data within the configuration offer messages; and responsive to said detecting step, unicasting host configuration requests from said server checker client to said unauthorized dynamic configuration server such that said unauthorized dynamic host configuration server is unable to respond to configuration requests from network clients. Independent claims 14 and 27 have been similarly amended.

Nothing in *Wasserman*, *Kaffine*, or *Lim*, individually or in any combination, discloses such a server checker client that draws (via broadcast) configuration server responses which are then analyzed for unauthorized server detection, and specifically targeting (i.e. unicasting) the detected unauthorized servers with configuration requests. Therefore, Applicants submit that claims 1, 14, 27 and all claims depending therefrom are patentably distinct from these as well as all other prior art references known to Applicants.

It is respectfully submitted that the pending claims have been placed in condition for allowance and favorable action is requested. No extension of time is believed to be required. However, in the event that an extension of time is required, please charge that extension fee and any other required fees to IBM Corporation Deposit Account Number 09-0457.

Applicant respectfully requests the Examiner contact the undersigned attorney of record at (512) 343-6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,

Matthew W. Baca
Reg. No. 42,277
DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
Telephone 512-343-6116
Facsimile 512-343-6446

ATTORNEY FOR APPLICANTS